centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1432

## Procedimiento de empleo seguro
## ARUBA OS-CX


Mayo de 2022

MINISTERIO DE DEFENSA

**Catálogo de Publicaciones de la Administración General del Estado**
**https://cpage.mpr.gob.es**

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.20 17:06:35 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-226-5

Fecha de Edición: mayo de 2022.

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

**AVISO LEGAL**

# ÍNDICE

# 1. INTRODUCCIÓN

1. Aruba CX es la última y más reciente familia de equipos de Aruba, para conmutación y enrutamiento de redes Ethernet, comúnmente conocidos como switches (aún cuando sean equipos que presten funciones de L2, L3 y capas superiores en algunos aspectos).
2. Esta familia de equipos, cubre necesidades desde acceso, equipos de agregación y equipos Datacenter.
3. La plataforma de conmutación Aruba CX, impulsada por el sistema operativo de red AOS-CX, simplifica las operaciones de red ofreciendo automatización, análisis distribuidos, seguridad y alta disponibilidad a las redes de campus y centros de datos. La arquitectura de microservicios en torno a la cual se construye AOS-CX ofrece análisis en toda la red y total programabilidad para permitir una garantía de red completa.
4. Los equipos han sido diseñados para poder ser explotados desde entornos locales (*on-premise*) y desde la cloud pública (*Aruba Central*, modalidad SaaS).

## 2. OBJETO Y ALCANCE

5. El propósito de este documento es proporcionar directrices de seguridad y mejores prácticas para las características y protocolos de gestión proporcionados por el **software Aruba OS-CX versión 10.06** y presentar configuraciones de ejemplo para ilustrar estas mejores prácticas.
6. Este documento por tanto, pone foco en las funcionalidades que pueden ser relevantes para una configuración segura del equipo, con el objetivo de que este no sea un vector de ataque. No pretende ser una guía de referencia completa de las características y comandos enumerados. Por lo que se recomienda que para ampliar el conocimiento y otras opciones de configuración, así como otra información adicional obtenga el último conjunto de manuales del software en el Portal de Soporte de Aruba (REF1).
7. Este documento describe mecanismos y funcionalidades relacionadas con los siguientes equipos de la familia de switches/routers Aruba CX:
    a) Equipos Datacenter
        - Aruba CX 8320.
        - Aruba CX 8325.
        - Aruba CX 8360.
        - Aruba CX 8400.
    b) Equipos Campus
        - Aruba CX 6200F.
        - Aruba CX 6300M.
        - Aruba CX 6300F.
        - Aruba CX 6405.

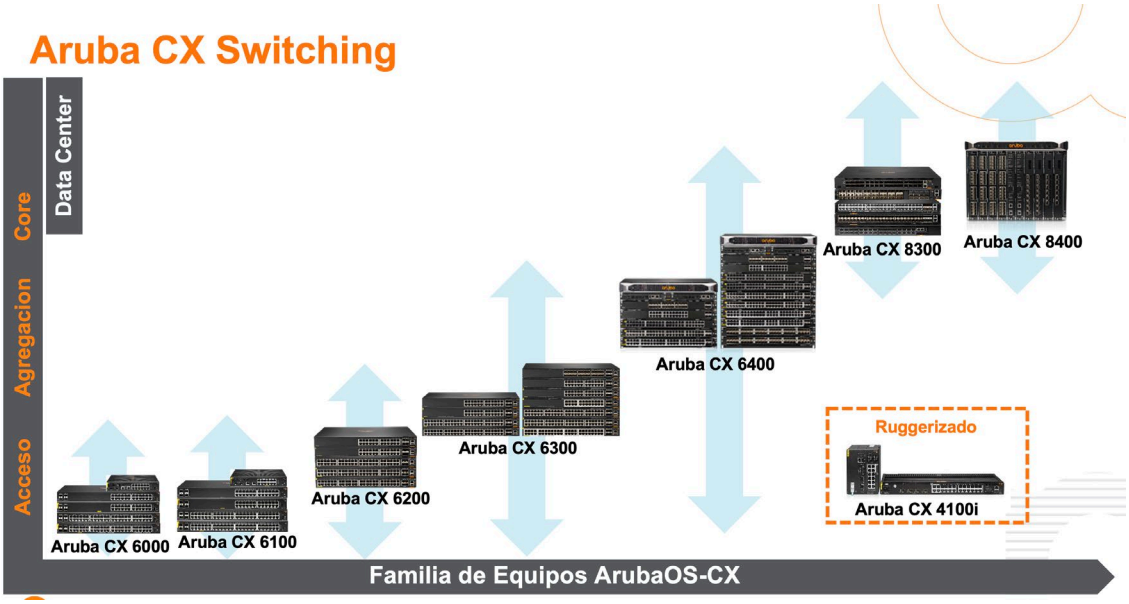


**Ilustración 1 Familia de Equipos Aruba-CX**

8. Como se verá en el documento, el equipo puede ser configurado de diferentes maneras. En este documento se describen los comandos y funcionalides que proporcionan la configuración segura del mismo, con independencia de cómo sea configurado.

## 3. ORGANIZACIÓN DEL DOCUMENTO

9. El presente documento se estructura en las secciones indicadas a continuación:

   a) **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   b) **Apartado 5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   c) **Apartado 6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) **Apartado 7**. En este apartado se recoge la lista de elementos que deben revisarse.

   e) **Apartado 8**. Referencias.

   f) **Apartado 9.** Abreviaturas.

# 4. FASE DE DESPLIEGUE E INSTALACIÓN

## 4.1 ENTREGA SEGURA DEL PRODUCTO

10. Los equipos Aruba OS-CX son dispositivos físicos que deben llegar al lugar de recepción perfectamente embalados y cerrados. Deben ir acompañados de un albarán de entrega que identifique los componentes contenidos en el envío. Debe comprobarse que las cajas lleguen cerradas y sin ningún tipo de daños.
11. Hay que tener en cuenta que algunos componentes del equipo pueden llegar en cajas separadas. Es necesario verificar que todos los componentes recibidos corresponden con el equipamiento pedido.
12. Todos los equipos así como sus componentes que puedan venir embalados en cajas separadas son perfectamente identificables mediante una etiqueta donde aparecen, entre otras informaciones, el código del equipo o componente y el número de serie del equipo ó componente.
13. Previamente a la instalación, es necesario verificar que todos los componentes del equipo han llegado correctamente embalados y etiquetados. Una vez abierta la caja del equipo, se debe verificar que, junto con el equipo, se encuentran:
    a) Kit de documentación.
    b) Adaptador USB Bluetooth que permite configurar el equipo desde un dispositivo móvil. Requiere la aplicación móvil Aruba CX. El adaptador se adjunta a una tarjeta en el kit de documentación.
    c) Cable de alimentación.
14. Es necesario tener en cuenta que, dependiendo del modelo de equipo y del tipo de instalación, se requiere de accesorios de montaje específicos que deben venir bien con el equipo o bien en un embalaje separado.
15. En caso de faltar algún componente o recibir alguna caja dañada o con indicios de haber sido abierta, ponerse inmediatamente en contacto con el fabricante.

## 4.2 ENTORNO DE INSTALACIÓN SEGURO

16. Los equipos Aruba OS-CX cubren una amplia gama de escenarios de trabajo, desde equipos de acceso para usuarios o dispositivos cableados a equipos de Centros de Proceso de Datos (CPD). Desde un punto de vista de la seguridad, el equipo puede securizarse sin necesidad de estar físicamente instalado en un CPD.
17. El lugar de instalación será típicamente un rack aunque ciertos modelos pueden instalarse en una superficie plana. El detalle de los entornos de montaje soportados se describe en la guía de instalación específica del equipo. Ver documento *Installation and Getting Started Guide* para cada modelo *REF4 – REF11*.

## 4.3 REGISTRO Y LICENCIAS

18. Los equipos de HPE Aruba de la gama Aruba OS-CX no necesitan estar registrados para disponer de su funcionalidad. No obstante, **se recomienda registrar los productos** para disfrutar de todas las ventajas y facilidades que brinda la posesión de un equipo, como notificaciones de seguridad, acceso a recursos como cliente, formaciones específicas para clientes registrados, etc.
19. Si se ha contratado el soporte del equipo, es necesario registrar ese soporte y los equipos bajo soporte en la plataforma ***Aruba Support Portal*** **-** *REF1*.
20. Como parte del contrato de soporte, se requiere que el *partner* de Aruba a través del cual se ha realizado la venta registre los números de serie del producto y que la ubicación de instalación se proporcione a Aruba.
21. El acceso a *Aruba Support Portal* (ASP) requiere disponer de una cuenta. Para crear una cuenta en ASP, hay que navegar a: https://asp.arubanetworks.com/
22. **Se recomienda que los miembros de la organización administradores del producto dispongan de una cuenta en ASP** para poder disponer de información relativa a parches, versiones de *firmware,* así como para la apertura de casos de soporte.
23. Se puede consultar el siguiente enlace para ver el detalle sobre cómo crear una cuenta ASP y cómo registrar los equipos: https://asp.arubanetworks.com/more-information. La creación de una cuenta en ASP puede tardar hasta un día laboral por motivos de verificación de la información.
24. ***Aruba Support Portal*** proporciona las siguientes capacidades.
    a) Gestión de casos en línea.
    b) Solicitar autorizaciones de devolución de materiales (RMA).
    c) Acceso a software, corrección de errores.
    d) Acceso a la documentación del producto.
    e) Acceso a base de conocimientos y *Airheads* en línea.
    f) *Aruba Solution Exchange* para asistencia en la configuración.
    g) Información sobre licencias.

## 4.4 CONSIDERACIONES PREVIAS

25. Antes de la instalación del equipo conviene tener en cuenta las consideraciones detalladas en este apartado.
26. Respecto de la alimentación del equipo, es conveniente que, en el caso de disponer de más de una fuente de alimentación, estas se conecten a líneas de alimentación diferentes dentro del rack. Si las fuentes de alimentación están conectadas a diferentes líneas de alimentación de corriente alterna, se puede suministrar energía redundante en caso de pérdida de una de las líneas de alimentación de corriente alterna.

27. Conviene también tener en cuenta si el equipo se va a montar con el chasis virtual o stack (VSF o VSX). En estos casos hay que preveer la distancia máxima a la que se podrán instalar los equipos que dependerá del tipo de interfaz utilizado para la comunicación entre ambos equipos (por ejemplo, interfaz RJ-45 o interfaz ópticom cables DAC). Ver apartado 5.14 ALTA DISPONIBILIDAD.

## 4.5 INSTALACIÓN

28. Los equipos se proporcionan con el sistema operativo instalado. La configuración inicial y actualización del *firmware* se detalla en el apartado 5 FASE DE CONFIGURACIÓN.

29. Respecto a la instalación física del equipo, se recomienda seguir los manuales correspondientes de cada modelo. Ver documento *Installation and Getting Started Guide* para cada modelo REF4 – REF11.

### 4.5.1 PRECAUCIONES DE INSTALACIÓN

30. Para proceder a instalar el equipo, se deben seguir los siguientes pasos generales. Para la instalación de un modelo específico se dispone de su correspondiente manual de instalación de detalle.

    a) Preparar el lugar de instalación. Asegurar que el entorno físico en el que instalará el equipo esté preparado correctamente, lo que incluye tener el cableado de red correcto listo para conectarse al equipo y tener una ubicación adecuada para el equipo.

    b) Instalar las fuentes de alimentación si aún no están instaladas.

    c) Instalar los conjuntos de ventiladores si aún no están instalados.

    d) Encender el equipo y verificar que los LED’s funcionen correctamente.

    e) Apagar el equipo.

    f) Montar el equipo. El equipo se puede montar en un bastidor de telecomunicaciones de 19 pulgadas o en una cabina de equipos.

    g) Instalar los transceptores si son necesarios. El equipo tiene ranuras para instalar transceptores de tipo SFP/SFP+/SFP28/QSFP+/QSFP28 dependiendo del modelo de equipo. Dependiendo de dónde instale el equipo, puede ser más fácil instalar los transceptores primero. Los transceptores se pueden intercambiar en caliente; se pueden instalar o quitar mientras el equipo está encendido.

    h) Conectar la alimentación al equipo. Una vez que el equipo esté montado, conectarlo a la fuente de alimentación principal.

    i) Conectar una consola de administración al equipo.

    j) Conectar los dispositivos de red. Con los cables de red adecuados, conectar los dispositivos de red a los puertos del conmutador.

31. En este punto, está completamente instalado. El equipo se entrega con una versión de sistema operativo previamente instalada. Por lo tanto puede arrancarse y es operativo.
32. El equipo arranca con la siguiente configuración básica por defecto:
    a) Todos los puertos asignados a VLAN1.
    b) Interfaz IP VLAN1 con asignación de IP por DHCP.
    c) Cuenta usuario *admin* sin contraseña asignada ni predeterminada. El equipo obligará a fijar una al arrancar, se deberán seguir las indicaciones del apartado 5.5.2.2 POLÍTICA DE CONTRASEÑAS.
33. A partir de este punto por tanto se puede proceder a la configuración inicial. Ver apartado 5.1 CONFIGURACION INICIAL.

## 4.6 CONEXION INICIAL

34. El equipo puede configurarse inicialmente mediante uno de los siguientes métodos:
    a) Puerto de consola serie. El detalle de esta conexión se puede consultar en el apartado *Initial configuration using the CLI* de la guía *AOS-CX 10.06 Fundamentals Guide - REF12.*
    b) Puerto *Ethernet* fuera de banda. El detalle de esta conexión se puede consultar en el apartado *Initial configuration using the CLI* de la guía *AOS-CX 10.06 Fundamentals Guide - REF12.* **Se recomienda hacer uso de este método para la conexión inicial con el dispositivo**.
    c) Zero Touch Provisioning (ZTP). El detalle de esta conexión se puede consultar en el apartado Initial configuration using ZTP de la guía AOS-CX 10.06 Fundamentals Guide - REF12.
    d) Aplicación Aruba CX. El detalle de esta conexión se puede consultar en el apartado *Initial configuration using the Aruba CX mobile app* de la guía *AOS-CX 10.06 Fundamentals Guide - REF12.*
35. En este documento se describen los comandos que proporcionan la configuración segura del mismo, con independencia de cómo sean insertados.

# 5. FASE DE CONFIGURACIÓN

## 5.1 CONFIGURACION INICIAL

### 5.1.1 PRIMERA CONEXION

36. En un estado predeterminado de fábrica, los dispositivos AOS-CX se entregan con el usuario predeterminado *admin* sin contraseña. Inmediatamente tras el primer acceso, y sin ninguna otra opción, se pide al usuario que cree una contraseña antes de darle acceso a la CLI. Para la creación de dicha contraseña, seguir las indicaciones del apartado 5.5.2.2 POLÍTICA DE CONTRASEÑAS.

37. Se muestra una captura para un modelo 6200F.

```
(C) Copyright 2017-2022 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
 Confidential computer software. Valid license from Hewlett Packard Enterprise
 Development LP required for possession, use or copying. Consistent with FAR
 12.211 and 12.212, Commercial Computer Software, Computer Software
 Documentation, and Technical Data for Commercial Items are licensed to the
 U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com


6200 login: admin
Password:[ENTER]


Please configure the 'admin' user account password.
Enter new password: *********
Confirm new password: *********
6200#
```

38. Es necesario identificar al equipo con un nombre de equipo. Para ello, utilizar el comando hostname.

```
hostname nombre_equipo
```

39. La interfaz de gestión integrada proporciona una forma de acceder y gestionar el conmutador que está separada del tráfico de producción. Las redes internas separadas del tráfico de producción suelen denominarse redes de gestión fuera de banda (OOBM).

40. En AOS-CX, la interfaz de gestión está lógicamente separada del resto del switch por medio de una única tabla virtual de enrutamiento y reenvío (VRF), denominada mgmt VRF.

41. El equipo presenta como configuración al menos dos VRFs: *Default* y Management

### 5.1.2 INTERFAZ DE GESTIÓN

42. El *mgmt VRF* (interfaz de gestión) es único en el sentido de que se asigna permanentemente al puerto físico de gestión y no puede asociarse a ninguna otra

interfaz del switch; el propio puerto de gestión no puede asociarse a ningún otro VRF.

43. La interfaz de gestión está habilitada por defecto para aprender una dirección IP a través de DHCP. **Se recomienda configurar la interfaz de gestión con una dirección IP estática, puerta de enlace y DNS.** Para ello, utilizar los siguientes comandos:

```
interface mgmt
  ip static 10.1.1.5/24
  default-gateway 10.1.1.1
  nameserver 10.0.1.10 10.0.1.11
```

44. Para mostrar el estado de la interfaz de gestión fuera de banda:

```
6200# show interface mgmt
  Address Mode                : static
  Admin State                 : up
  Link State                  : down
  Mac Address                 : b8:d4:e7:xx:xx:xx
  IPv4 address/subnet-mask    : 10.1.1.5/24
  Default gateway IPv4        : 10.1.1.1
  IPv6 address/prefix         :
  IPv6 link local address/prefix:
  Default gateway IPv6        :
  Primary Nameserver          : 10.0.1.10
  Secondary Nameserver        : 10.0.1.11
  Tertiary Nameserver         :
  6200#
```

### 5.1.3 *VRF DEFAULT*

45. El VRF Default se asocia automáticamente con todas las interfaces que no son de gestión, incluidos los puertos enrutados de capa 3, los puertos no enrutados y las interfaces VLAN conmutadas (SVI) creadas en el conmutador, a menos que la interfaz esté explícitamente unida a otro VRF.

46. Los siguientes servicios de gestión están habilitados por defecto en un conmutador Aruba CX:

    a) SSH en el puerto TCP 22.

b) HTTP/HTTPS y API REST de lectura/escritura en los puertos TCP 80 y 443. **Se recomienda deshabilitar estos servicios**, tal como se muestra en el apartado 5.7 CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS.

47. Los conmutadores Aruba CX 8320, 8325, 8360 y 8400 se envían con estos servicios habilitados solo en el VRF de gestión, mientras que los conmutadores 6200, 6300 y 6400 se envían con estos servicios habilitados tanto en el VRF por defecto como en el de gestión.
48. Se recomienda gestionar los dispositivos, siempre que sea posible, desde la red de gestión dedicada.

### 5.1.4 ASISTENTE GENERADOR CONFIGURACIONES

49. Con objeto de facilitar la configuración inicial, se ha generado un asistente de configuraciones basados en este documento.
50. Este asistente es alcanzable desde la siguiente URL:

    https://ase.arubanetworks.com/solutions/id/289

51. Este asistente solicita diferentes valores con los cuales genera una configuración de referencia para la configuración inicial.
52. Para acceder a esta herramienta es necesario hacer uso de credenciales de usuario de la comunidad de *Aruba Support Portal ASP - REF1.*

## 5.2 MODO DE OPERACIÓN SEGURO

53. El sistema operativo AOS-CX proporciona acceso al sistema *Linux* subyacente, permitiendo a los administradores lanzar una sesión de *shell Bash* desde la línea de comandos del switch.
54. Por defecto, todas las cuentas que forman parte del grupo de administradores pueden acceder al *shell* utilizando el comando *start-shell*, y pueden utilizar el comando *sudo* para ejecutar comandos del *shell* con permisos de *root*. Esto permite proporcionar herramientas avanzadas de *troubleshooting*.
55. El uso indebido del acceso al *shell* podría dar lugar a la divulgación del tráfico de red sensible a un tercero no autorizado a través de la duplicación de paquetes a un dispositivo remoto, o podría causar una denegación de servicio mediante la modificación o eliminación de los archivos del sistema y hacer que el dispositivo no pueda arrancar, requiriendo la restauración del software a través de la consola de *ServiceOS*.
56. El acceso al *shell Bash* se puede deshabilitar completamente cambiando el modo de seguridad del switch. AOS-CX proporciona dos (2) modos de seguridad que controlan el acceso a la consola del *ServiceOS*: *standard y enhanced*.
57. Todos los conmutadores Aruba CX funcionan en modo *standard* por defecto, sin restricciones a nivel de sistema para ninguna funcionalidad. El modo de seguridad

mejorado (*enhanced*) desactiva el acceso al comando *start-shell* en la CLI de AOS-CX, así como los comandos de *ServiceOS config-clear*, *password*, *sh* y *update*.

58. El cambio del modo de seguridad del conmutador se realiza desde el *shell* de *ServiceOS*, que requiere una conexión de consola al conmutador. Todos los cambios en el modo de seguridad del conmutador (de *standard* a *enhanced*, o de *enhanced* a *standard*) tienen como resultado la puesta a cero del sistema de archivos y el restablecimiento de los valores predeterminados de fábrica.
59. Para realizar el cambio de modo, ejecutar el siguiente comando para resetear el equipo en modo ServiceOS.

    *switch# boot system serviceos*

    *One time boot to ServiceOS initiated.*

    *Checking if the configuration needs to be saved...*

    *This will reboot the system to ServiceOS and render*

    *the entire switch unavailable.*

    *Access to ServiceOS is only available through the serial console.*

    *Continue (y/n)?*

60. Una vez que el conmutador se haya reiniciado y se muestre el indicador de inicio de sesión de ServiceOS, iniciar sesión como admin. Se debe utilizar el siguiente comando para activar el modo de seguridad mejorado:

    *SVOS> secure-mode enhanced*

    *################################WARNING################################*

    *This will set the switch into enhanced secure mode. Before*

    *enhanced secure mode is enabled, the switch must securely erase*

    *all customer data and reset the switch to factory defaults.*

    *This will initiate a reboot and render the switch unavailable*

    *until the zeroization is complete.*

    *################################WARNING################################*

    *Continue (y/n)?*

61. Hacer clic en *y* para confirmar. El dispositivo se reiniciará con valores de fábrica. **Se debe hacer uso del dispositivo en modo *enhanced*.**

## 5.3 CONTRASEÑA DE ACCESO A SERVICEOS

62. Por defecto, el shell de ServiceOS (accesible solo desde el puerto de consola del conmutador local) no requiere ninguna contraseña para iniciar sesión como admin; para habilitar la autenticación con contraseña para ServiceOS, utilizar el siguiente comando desde el contexto de configuración:

*switch(config)# system serviceos password-prompt*

63. Cuando este ajuste está activado, el inicio de sesión en el *shell* de *ServiceOS* con el usuario administrador requiere la misma contraseña utilizada para autenticar al usuario administrador en la CLI o la interfaz de usuario web de AOS-CX. **Se debe activar esta opción**.

64. Si este ajuste está activado, no se puede restablecer mediante ServiceOS una contraseña de usuario administrador olvidada; si no hay otras cuentas de usuario con acceso de nivel de administrador, el conmutador debe ponerse a fábrica, ver apartado 5.16 RESETEO A FABRICA (*FACTORY DEFAULTS*).

## 5.4 AUTENTICACIÓN

65. El producto dispone de las siguientes opciones para la autenticación de los usuarios:
    - Autenticación local con credenciales locales.
    - Autenticación remota a través de servidores externos RADIUS y TACACS+.

66. En la autenticación de usuarios, se recomienda hacer uso únicamente de la autenticación local y deshabilitar la autenticación remota. Para ello:

    *switch(config)# aaa authentication login default local*

67. El producto realiza autenticación de los dispositivos en el acceso a los puertos, mediante *eap-radius*. Ver apartado 5.15 CONTROL DE ACCESO A LA RED.

## 5.5 ADMINISTRACIÓN DEL PRODUCTO

### 5.5.1 ADMINISTRACIÓN LOCAL Y REMOTA

68. El producto dispone de los siguientes métodos para la administración:
    - Administración local mediante puerto USB-C.
    - Administración remota a través de SSH. **Se recomienda el uso de este método para realizar la configuración y gestión del producto**.
    - Administración remota a través de HTTPS. **No se recomienda el uso de este método.**
    - Administración remota a través de API REST. **No se recomienda el uso de este método.**
    - Gestión Nube o *Cloud*. Esta gestión se realiza mediante la apliación *Aruba Central*, en modalidad *Software-as-a-Service* (SaaS). **No se recomienda el uso de este método, dado que las funcionalidades de seguridad de *Aruba Central* no han sido evaluadas.**

69. El detalle de cómo desactivar los protocolos no recomendados, así como asegurar el acceso mediante SSH se puede consultar en el apartado 5.7 CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS.

### 5.5.2 CONFIGURACIÓN DE ADMINISTRADORES

#### 5.5.2.1 AUTENTICACION LOCAL

70. El producto hace uso grupos para definir los permisos de los que dispondrán los usuarios. Las cuentas de usuario local deben asignarse a un grupo. El producto dispone por defecto de tres grupos predefinidos:

    - Administradores: acceso completo.
    - Operadores: acceso limitado.
        - Acceso *Display-Only*.
        - Ver información no sensible de la configuración.
        - Solo método GET a través de la REST API.
    - Auditores: acceso limitado.
        - Acceso CLI al contexto *auditors* únicamente.

71. Para crear nuevos usuarios y asignarles un grupo, utilizar el siguiente comando:

```
switch(config)# user <USERNAME> group {administrators | operators | auditors | <USER-GROUP>} password [ciphertext <CIPHERTEXT-PASSWORD> | plaintext <PLAINTEXT-PASSWORD>]
```

72. La contraseña puede ser introducida en formato texto claro o cifrado. Se alamacenará siempre cifrada y en la configuración se mostrará en formato cifrado (lo cual facilita el registro de configuraciones con estas deficiones incluidas, sin revelar las contraseñas).

73. La configuración de un usuario con contraseña introducida en texto en claro:

```
switch(config)# user localoperator group operators password plaintext I-h@ve-Read-0n1y-Acc3ss!
```

74. Este ejemplo se mostraría de la siguiente forma en la configuración:

```
user localoperator group operators password ciphertext AQBapRgGuzC/qTH+7cA5hJg2a/y6EjLJ5Vdivf5ofGzvdkGAYgAAAP/DtjEY/s2psoMkNxWqhN2f+4tibBwEMraRn+MOSbyfx1sdMq9Ii/8+641RGYnDNS9zzDEMlmUIiiiGHPptfFaVnM57BEvwxjNLR+IGpYJ9VnYksH+zLPmPJPhM3duWgP
```

75. El campo usuario tiene como máximo una longitud de 32 caracteres y no puede contener ciertos nombres Linux reservados. La longitud de contraseñas máxima será también de 32 caracteres.

76. Para visualizar los grupos de usuarios o nombres de usuarios utilizar el siguiente comando:

```
show user-group [<GROUP-NAME>] [vsx-peer]
show user information
show user-list [vsx-peer]
```

77. Los grupos definidos manualmente, permiten especificar qué comandos pueden utilizar y cuales no los usuarios pertenecientes al grupo.

78. El detalle de configuración de los usuarios y roles locales en los dispositivos se puede consultar en el capítulo Managing local users and groups, de la guía *AOS-CX 10.06 Security Guide – REF13.*

#### 5.5.2.2 POLÍTICA DE CONTRASEÑAS

79. El produto permite definir criterios de complejidad para las contraseñas de usuarios locales. Estas se pueden definir haciendo uso del comando *password complexity*:

```
switch(config)# password complexity
switch(config-pwd-cplx)# history-count 5
switch(config-pwd-cplx)# minimum-length 12
switch(config-pwd-cplx)# position-changes 10
switch(config-pwd-cplx)# lowercase-count 1
switch(config-pwd-cplx)# uppercase-count 1
switch(config-pwd-cplx)# numeric-count 1
switch(config-pwd-cplx)# special-char-count 1
switch(config-pwd-cplx)# enable
switch# exit
```

80. Dispone de las siguientes opciones:

    a) *History count*: Impide reutilización de las contraseñas anteriores. **Se debe utilizar un valor de 5 contraseñas**.

    b) *Position-Change*: define cuánto debe diferir una nueva contraseña de la anterior.

    c) *Minimum-length*: define la longitud minima de las contraseñas. **Se debe utilizar un valor de, al menos, 12 caracteres**.

    d) *Lowercase-count, uppercase-count, numeric-count, special-char-count*: Definen el número de minúsculas, mayúsculas, números y caracteres especiales respectivametne que deben contener las contraseñas. **Se debe definir un valor de, al menos, uno para cada parámetro.**

81. Adicionalmente, el administrador deberá asegurar los siguientes parámetros relativos a las contraseñas de manera procedural:

    **a) Realizar cambios de contraseñas cada 60 días.**

    **b) No permitir un nuevo cambio de contraseña hasta pasados 10 días.**

#### 5.5.2.3 PARÁMETROS DE SESIÓN

82. El producto permite establecer un número máximo de sesiones de gestión CLI concurrentes por usuario, así como un tiempo de espera de la sesión que cerrará automáticamente una sesión CLI después de un período de inactividad.

83. Por defecto, AOS-CX permite hasta 5 sesiones CLI concurrentes para cada cuenta de usuario. Este valor se puede cambiar desde el contexto *cli-session* con el comando *max-per-user*. **Se recomienda establecer un valor de una única sesión concurrente por usuario:**

    *switch(config)# cli-session*

    *switch(config-cli-session)# max-per-user 1*

84. Se puede definir también un periodo de inactividad tras el cual los usuarios deberán reautenticarse. Por defecto, el tiempo de espera de la sesión CLI se establece en 30

minutos. **Se debe configurar un valor de 5 minutos**. Para ello, desde el contexto *cli-session* utilizar el comando *timeout*:

*switch(config-cli-session)# timeout 5*

85. Se puede limitar el número de intentos de *login* fallidos para autenticaciones locales, así como el periodo de bloqueo tras el número de fallos. **Se debe configurar un valor de 3 intentos fallidos y 5 minutos de espera** mediante el siguiente comando:

```
switch(config)# aaa authentication limit-login-attempts <ATTEMPTS> lockout-time <LOCKOUT-TIME>
```

#### 5.5.2.4 *BANNER* DE ACCESO

86. **Se debe configurar un mensaje de acceso al sistema**. Para ello utilizar el siguiente comando, de tal forma que el mensaje configurado se mostrará antes de realizar el acceso al sistema:

```
switch(config)# banner motd %
Enter a new banner. Terminate the banner with the delimiter you have chosen.
switch(config-banner-motd)# ================================
switch(config-banner-motd)#         Este es un sistema privado
switch(config-banner-motd)#. Abandone la conexión si no esta autorizado.
switch(config-banner-motd)# ================================
switch(config-banner-motd)# %
```

## 5.6 CONFIGURACIÓN DE PUERTOS

### 5.6.1 VLAN EN PUERTOS

87. Cada puerto de un conmutador debe pertenecer a, al menos, una VLAN. El tráfico enviado por los sistemas conectados a cada VLAN queda confinado en esa VLAN: cada VLAN constituye un dominio de *broadcast* diferente. En este sentido, el uso de VLAN permite reducir el tráfico de difusión en las redes, confinando a cada VLAN los efectos de los problemas tales como las tormentas de *broadcast*.

88. Un puerto puede pertenecer a varias VLAN distintas, en cuyo caso se debe configurar en modo etiquetado. Es el caso habitual de los enlaces entre conmutadores o de los puertos conectados a servidores. Los puertos conectados a sistemas de usuarios suelen pertenecer a una única VLAN y estar configurados en modo no etiquetado.

89. Las VLAN pueden expandirse a varios conmutadores, de forma que sistemas conectados a conmutadores distintos pueden pertenecer a la misma VLAN.

90. La conexión entre VLAN debe realizarse a nivel 3, mediante *routers* externos o servicios de encaminamiento implementados en los propios conmutadores. En ArubaOS-CX, la configuración inicial del equipo consta de una única VLAN ya creada (VLAN 1), a la que pertenecen por defecto todos los interfaces. Para evitar posibles problemas en la red cuando se interconectan *switches*, **es recomendable no utilizar dicha VLAN y crear una nueva VLAN en la que se agrupen todos los puertos inactivos**.

91. Cuando se configuran las VLANs y los puertos que pertenecen a ella hay que tener especial cuidado en introducir estrictamente los puertos que se hayan considerado de uso necesario.

92. El detalle de configuración de las VLAN en los dispositivos se puede consultar en el capítulo *VLANs*, de la guía *AOS-CX 10.06 Fundamentals Guide – REF12*.

### 5.6.2 APAGADO DE PUERTOS.

93. **Se deben deshabilitar todos aquellos puertos del dispositivo que no se estén utilizando**, con el objeto de evitar conexiones o accesos no autorizados a dichos puertos.

94. Para bloquear o cerrar los puertos no utilizados, utilizar los siguientes comandos:

```
switch(config)# interface <interface>
switch(config-if)#  [no] shutdown
```

95. Para conocer el estado de los puertos se puede utilizar el comando:

```
show interface brief
```

### 5.6.3 LIMITE DE MAC POR PUERTO

96. ArubaOS-CX proporciona medidas específicas para poder configurar la seguridad a nivel de puerto de una forma precisa y, así, definir qué equipos (direcciones MAC) pueden conectarse o limitar el número máximo de equipos que se conectan a cada puerto.

97. Permite, además, configurar la generación de alarmas o incluso el bloqueo de los puertos en caso de que se detecten accesos no permitidos.

98. Cuando se activa el control de seguridad en un puerto, se puede configurar:

    a) La activación de forma global en la configuración.

        *port-access port-security enable*

    b) El número máximo de direcciones MAC permitidas, mediante el comando *client-limit* dentro del interfaz.

        *interface 1/1/2*

        *no shutdown*

        *no routing*

        *vlan access 1*

        *port-access port-security*

        *client-limit 2*

    c) Las direcciones MAC permitidas. Se configuran mediante el comando *mac-address* dentro del interfaz.

```
interface 1/1/3
   no shutdown
   no routing
   vlan access 1
   port-access port-security
      mac-address aa:bb:cc:dd:ee:01
      mac-address aa:bb:cc:dd:ee:02
```

99. Es importante tener en cuenta que las direcciones MAC aprendidas de forma dinámica se almacenan en la tabla de filtrado del *switch* durante un tiempo máximo (unos minutos típicamente) siguiendo el algoritmo estándar de los conmutadores *Ethernet*. Además, si el conmutador se reinicia se eliminan. Por el contrario, las direcciones configuradas de forma estática se añaden a la configuración del conmutador, por lo que se conservan en la tabla de filtrado tras un rearranque del equipo.

100. El detalle de configuración de los la protección mac en los dispositivos se puede consultar en el capítulo *Port security*, de la guía *AOS-CX 10.06 Security Guide – REF13*.

### 5.6.4 LIMITACION DE TRAFICO DE *BROADCAST*

101. Una tormenta de broadcast consiste en la presencia de un volumen de tráfico excesivo enviado a la dirección de difusión (*broadcast*) de la LAN. Dado que por definición el tráfico enviado a broadcast debe ser replicado en todos los puertos del conmutador, esto puede provocar un consumo excesivo de recursos del equipo y de ancho de banda de la red para hacer frente a este tráfico. En casos graves, incluso puede causar el colapso total del conmutador y de la red.

102. Para prevenir este tipo de ataques o los efectos de una configuración errónea, **es importante implementar medidas que limiten el tráfico de tipo *broadcast***, de forma que nunca llegue a consumir todos los recursos de la red y quede un margen para que el que el equipo pueda seguir teniendo conectividad y no se quede aislado.

103. ArubaOS-CX proporciona comandos para limitar el ancho de banda consumido por el tráfico de difusión. La configuración se realiza para cada puerto del conmutador, por lo que se pueden implementar politicas de limitación distintas para cada tipo de interfaz (acceso, *inter-switch*, etc.).

104. Para limitar el ancho de banda consumido por el tráfico de difusión en un puerto, utilizar el siguiente comando:

```
rate-limit {broadcast | multicast | unknown-unicast} <RATE> pps
```

105. Por ejemplo, para limitar 4000pps el tráfico de difusión que entra por el interfaz 3:

```
switch(config)# interface 1/3/3
switch(config-if)# rate-limit multicast 4000 pps
```

106. Se recomienda limitar el tráfico de difusión a un valor entre el 5% y el 10% de los paquetes por segundo totales necesarios para la organización.

### 5.6.5 PROTECCION FRENTE A ENVIO DE MENSAJES DE CONTROL STP

107. Cuando se utiliza el protocolo *Spanning Tree* (STP) en una red compuesta por varios conmutadores es muy importante protegerse frente al posible envío de mensajes de control (BPDU) falsos generados desde los puertos de acceso a la red.

108. Existen múltiples ataques documentados que mediante el envío de estas BPDUs falsas permiten redirigir la información hacia sistemas fraudulentos (ataques *man-in-the-middle*) o simplemente interrumpir el servicio (ataques de denegación de servicio).

109. Es por ello **imprescindible proteger los conmutadores para que solo acepten BPDUs procedentes de los puertos que los conectan con otros conmutadores** y descartar todas aquellas BPDUs recibidas a través de puertos de acceso.

110. Para activar la protección frente al envío de BPDUs en un conjunto de puertos, se debe utilizar el siguiente comando:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree bpdu-guard
```

111. Una vez activado el comando, si se recibe una BPDU por alguno de los puertos especificados, se descartará la BPDU y se deshabilitará el puerto.

112. Adicionalmente, es posible generar una alarma (*trap*) de SNMP para avisar al gestor de red del evento detectado. Para ello hay que ejecutar el comando:

```
spanning-tree trap {new-root|topology-change [instance <0-64>] | errant-bpdu | root-guard-inconsistency | loop-guard-inconsistency}
switch(config)# spanning-tree trap errant-bpdu
```

113. Para ver la configuración relativa a la protección frente a envío de BPDUs se puede ejecutar el comando:

```
show spanning-tree detail
```

### 5.6.6 LISTAS DE ACCESO

114. Las listas de acceso (*Access Control List* o ACL) son un método de filtrado de flujos de datos. Pueden ser usadas para restringir el acceso a la gestión del equipo y para realizar el filtrado de tráfico que atraviesa el equipo. Aplicadas a los conmutadores, las ACLs se basan en un conjunto de reglas básicas (*Access Control Entries* o ACE) que determinan la autorización (reglas de tipo *permit*) o denegación (reglas de tipo *deny*) del tráfico en función de campos de las cabeceras de los paquetes tales como las direcciones IP y puertos, tanto origen como destino, o el protocolo.

115. Por cada paquete recibido, las reglas que componen una ACL se evalúan línea a línea hasta que se encuentra una coincidencia. Por esta razón, hay que definir primero las reglas más específicas y posteriormente las más generales. Es importante

recordar que las listas de acceso tienen una denegación implícita al final (todo el tráfico se filtra por defecto salvo que se permita explicitamente).

116. El detalle de configuración de listas de acceso se puede consultar la guía *AOS-CX 10.06 ACLs and Clasiffier Policies Guide– REF14*.

## 5.7 CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS

### 5.7.1 TRANSFERENCIA DE ARCHIVOS

117. **Para la transferencia de ficheros se debe hacer uso de SFTP**. Se soporta TFTP por compatibilidad histórica con servicios de gestión, pero no debe utilizarse a no ser que sea estrictamente necesario. Por ejemplo para subir una imagen mediante SFTP sería:

```
switch# copy sftp://sftpuser@10.10.10.1/TL_10_01_0001.swi primary vrf mgmt
```

### 5.7.2 PUERTO USB

118. En los equipo tipo chasis, se puede controlar el uso de puerto USB para almacenamiento externo. El puerto USB se deshabilita de la siguiente manera:

```
switch(config)# no usb
```

119. En caso de querer habilitarlo nuevamente, utilizar el comando sin el prefijo *no*.

### 5.7.3 SERVIDOR SSH

120. El acceso remoto mediante SSH utiliza, siempre, al menos SSH v2.0. El servidor SSH regenera las claves utilizadas para todas las sesiones SSH abiertas cada hora o cada 1GB de datos transferido, lo que ocurra primero. Estos valores no son configurables.

121. Se deberán configurar los siguientes parámetros para asegurar un empleo seguro del protocolo SSH:

a) Verificar que el servidor SSH está habilitado:

*ssh server vrf mgmt*

b) Generar la clave del servidor. Para ello utilizar el siguiente comando, **se deben utilizar únicamente los siguientes algoritmos**:

*ssh host-key [ecdsa [ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | ecdsa-sha2-nistp521]]*

c) Es posible permitir la autenticación mediante claves públicas. Para ello, utilizar el siguiente comando para asociar una clave a un usuario:

*user <username> authorized-key <authorized_key>*

d) En caso de no utilizar este tipo de autenticación, deshabilitarlo:

*no ssh public-key-authentication*

e) Habilitar únicamente el uso de algoritmos seguros:

*switch(config)# ssh ciphers aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc*

*switch(config)# ssh macs hmac-sha2-256, hmac-sha2-512, hmac-sha1*

*switch(config)# ssh key-exchange-algorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384*

*switch(config)# ssh host-key-algorithms ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521*

*switch(config)# ssh public-key-algorithms ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521*

### 5.7.4 SERVIDOR HTTP

122. No se dispone de servidor HTTP. El puerto 80 se implementa para redireccionar al puerto HTTPS (443).

### 5.7.5 SERVIDOR HTTPS

123. El servidor HTTPS proporciona acceso tanto al interfaz gráfico, como a la REST API. El interfaz gráfico incluye el motor análisis de red (*Network Analytics Engine*, NAE).

124. Se recomienda administrar el producto a través de la interfaz CLI mediante SSH. Por ello, se recomienda deshabilitar el servidor HTTPS, para ello hacer uso del siguiente comando:

```
switch# config
switch(config)# no https-server vrf mgmt
```

125. Para ver estado de configuración del servidor HTTPS, utilizar el siguiente comando:

```
switch# show https-server
HTTPS Server Configuration
--------------------------
VRF : default, mgmt
REST Access Mode : read-write
Max sessions per user : 6
Session timeout : 20
```

### 5.7.6 SNMP

126. En relación a procolos de gestión SNMP, el producto dispone de las versiones v1, v2 y v3, estando por defecto todas ellas dehabilitadas.

127. Se recomienda utilizar SNMP únicamente cuando sea necesario. Para evitar que la información SNMP se transmita en texto plano **se recomienda utilizar únicamente la versión 3 de SNMP.**

128. SNMP se encuentra deshabilitado por defecto. En caso de habilitarlo y querer deshabilitarlo posteriormente, utilizar los siguientes comandos:

```
Aruba-CX(config)# no snmp-server vrf <VRF-NAME>
Aruba-CX(config)# no snmp-server snmpv3-only
Aruba-CX(config)# no snmpv3 user usuario_snmp
Aruba-CX(config)# no snmp-server host <IP>
```

129. Los pasos a seguir para configurar SNMP versión 3 son los siguientes:

a) Habilitar SNMP en una instancia VRF.

```
Aruba-CX(config)# snmp-server vrf <VRF-NAME>
```

b) Definir el contacto, localización y descripción del switch (opcional).

```
Aruba-CX(config)# snmp-server system-contact <Contacto>
Aruba-CX(config)# snmp-server system-location <Localizacion>
Aruba-CX(config)# snmp-server system-description <Descripcion>
```

c) Deshabilar el uso de SNMP V2 y V1.

```
Aruba-CX(config)# snmp-server snmpv3-only
```

d) Definir un usuario SNMP V3.

```
Aruba-CX(config)# snmpv3 user usuario_snmp auth sha auth-pass plaintext <SHA-TEXT>
priv aes priv-pass plaintext <AES-TEXT>
```

e) Crear un contexto SNMP V3.

```
Aruba-CX(config)# snmpv3 context <Contexto> vrf <VRF-NAME> community <Comunidad>
```

130. Por otro lado, si se enviarán traps, se definen de la siguiente forma.

```
Aruba-CX(config)# snmp-server host <IP> trap version v3 user <Usuario> vrf <VRF-NAME>
```

131. Indicar que, en los switches Aruba de la gama CX, SNMP solo tiene propiedades de lectura.

### 5.7.7 DESACTIVACIÓN ARUBA CENTRAL

132. *Aruba Central* es una consola de gestión de los dispositivos desde la nube. Dado que este componente no ha formado parte de la evaluación de seguridad, **se debe deshabilitar esta función**.

133. Para ello, utilizar los siguientes comandos:

```
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

### 5.7.8 DESACTIVACION *BLUETOOTH*

134. Los dispositivos cuentan con la funcionalidad bluetooth. **Se debe desactivar esta funcionalidad** y habilitarla únicamente cuando vaya a utilizarse.

*switch(config)# bluetooth disable*

*switch# show bluetooth*

*Enabled : No*

*Device name : <XXXX>-<NNNNNNNNNN>*

## 5.8 GESTIÓN DE CERTIFICADOS

135. El producto requiere la instalación y configuración de certificados para las comunicaciones con el servidor externo de auditoría. **Deberán utilizarse certificados de una Autoridad de Certificación (CA) de confianza**, evitando el uso de certificados autofirmados.

136. El detalle de configuración de los certificados del producto se puede consultar en el apartado *PKI* de la guía *AOS-CX 10.06 Security Guide – REF13*.

137. Deberán seguirse los siguientes pasos generales:

- Instalar el certificado de la CA raíz que firmará el certificado del producto, así como el certificado de la CA del servidor *syslog* externo.
- Generar una CSR (*Certificate Signing Request*), para crear el certificado que usará el producto. **Se deberá utilizar uno de los siguientes parámetros para la creación del certificado**:
    - Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256.
    - Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.
- Importar el certificado una vez obtenido.

## 5.9 SINCRONIZACIÓN HORARIA

138. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.**

139. Los equipos ArubaCX soportan la sincronización del reloj interno con servidores de hora externos mediante los protocolos TimeP y NTP (*Network Time Protocol*).

140. Los pasos para configurar el servicio NTP en el producto son los siguientes:

a) Habilitar autenticación NTP.

*Aruba-CX(config)# ntp authentication*

b) Configurar las claves de autenticación, así como su identificador y el tipo de cifrado. El producto solo dispone de MD5 y SHA1. Aunque ninguno de los métodos es considerado suficientemente robusto, **se debe usar SHA1**.

*Aruba-CX(config)# ntp authentication-key <KEY-ID> {md5 | sha1} <PASSWORD> [trusted]*

c) Definir los servidores NTP hasta un máximo de 8 servidores, por lo que se podrá repetir este comando tantas veces como se desee hasta completar los 8 y pudiendo definir alguno de ellos como preferido.

*Aruba-CX(config)# ntp server <IP-ADDR> [key <KEY-NUM] [prefer]*

d) Definir la instancia VRF que se utilizara para establecer la conexión con el servidor NTP y actualizar así el dispositivo.

*Aruba-CX(config)# ntp vrf <VRF-NAME>*

e) Habilitar NTP. Esta opción está habilitada por defecto.

*Aruba-CX(config)# ntp enable*

141. Finalmente se puede verificar la configuración NTP con el siguiente comando:

```
Aruba-CX(config)# show ntp status
NTP Status Information

NTP                         : Enabled
NTP Authentication          : Enabled
NTP Server Connections      : Using the default VRF

System time                 : Mon May 10 15:13:23 CEST 2021
NTP uptime                  : 1 days, 3 hours, 17 minutes, 25 seconds

NTP Synchronization Information

NTP Server                  : 192.168.2.116 at stratum 4
Poll interval               : 1024 seconds
Time accuracy               : Within 0.006468 seconds
Reference time              : Mon May 10 2021 14:49:25.970 as per Europe/Madrid
```

142. Comando para verificar los sincronizadores de tiempo a los que está vinculado el dispositivo:

```
Aruba-CX(config)# show ntp associations
-------------------------------------------------------------------------------
 ID                      NAME          REMOTE          REF-ID ST LAST POLL REACH
-------------------------------------------------------------------------------
* 1             DC-01.lab.com   192.168.2.116 162.159.200.123  4  705 1024   377
+ 2       time.cloudflare.com 162.159.200.123     10.40.9.201  3  596 1024   377
-------------------------------------------------------------------------------
```

143. Para mostrar las claves de autenticación definidas:

```
Aruba-CX(config)# show ntp authentication-keys
-------------------------------------------------------------------------------------------
-----
Key ID   Trusted   Type    Encrypted Key
-------------------------------------------------------------------------------------------
-----
1        No        SHA1
AQBapbhBuAX7PxpenrLcFfk5xBiD9K4+wnZHKu1/mqxewNs0CgAAAJaTpzSrC9NI3yE=
```

## 5.10 ACTUALIZACIONES

144. **La actualización del producto debe realizarse con la mayor celeridad posible** y llevarse a cabo manualmente por parte de un usuario administrador. Este deberá realizar la descarga de la versión deseada desde la siguiente página:

*https://asp.arubanetworks.com/downloads*

145. En esa misma web el administrador puede subscribirse a notificaciones de nuevas versiones de *software*, así como otro tipo de notificaciones (producto, seguridad y documentación).

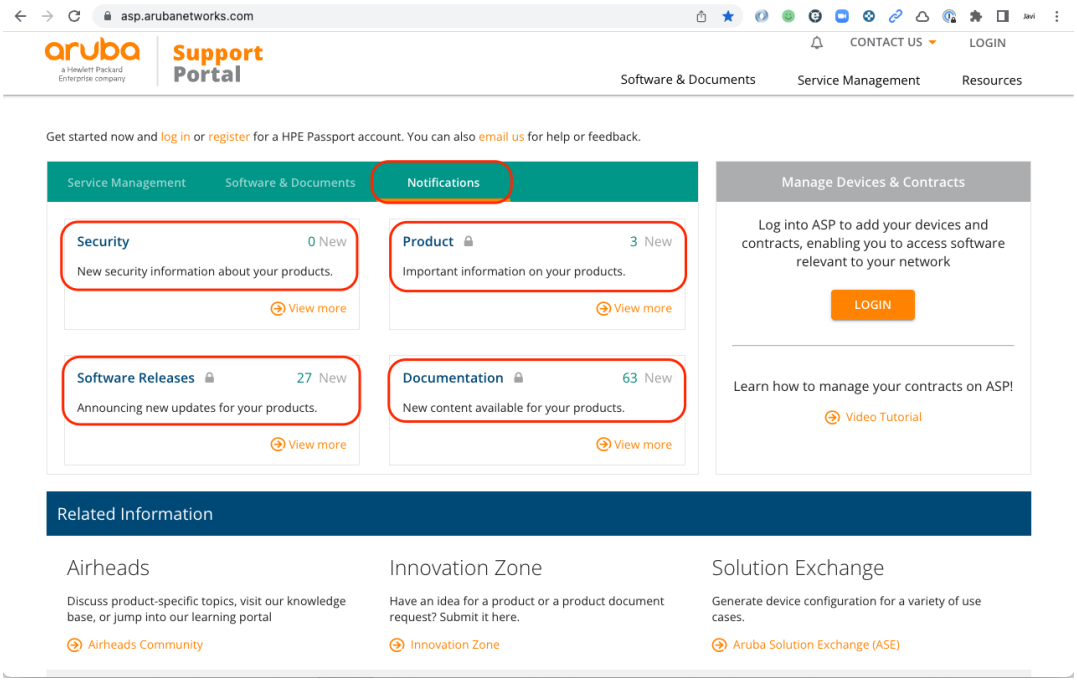


**Ilustración 2. Notificaciones en portal de soporte.**

146. Una vez descargada la versión, **se debe verificar el hash SHA256 del fichero**. Para ello realizar el hash del fichero y comprobar que coincide con el mostrado en la página de descarga, en el apartado *SHA256*.

147. Los switches disponen de dos localizaciones para su *software* (*firmware*), una partición llamada "*Primary*" y otra "*Secondary*", por lo que habrá que especificar cual de las dos particiones se quiere actualizar en cada momento.

148. Se deberá utilizar SFTP para realizar la transmisión del software al switch de manera segura.

149. También se dispone de la posibilidad de trasmitir el software de manera local mediante el puerto USB tipo A.

150. El comando para la actualización del software del switch mediante el uso de un servidor de ficheros es el siguiente:

```
Aruba-CX(config)# copy <REMOTE-URL> {primary | secondary} [vrf <VRF-NAME>]
```

151. Donde *<REMOTE-URL>* es la dirección del servidor de ficheros en el siguiente formato para una conexión SFTP:

```
sftp://<USERNAME>@<IP-ADDR>[:<PORT-NUM>]/<FILENAME>
```

152. El comando para una actualización local del *software* a través de un usb sería:

```
Aruba-CX(config)# copy usb:/file {primary | secondary}
```

153. Adicionalmente, el *firmware* es firmado por Aruba. El dispositivo verifica automáticamente esta firma durante la instalación. Si la comprobación es correcta, se devolverá el siguiente mensaje.

```
This operation will overwrite the primary firmware image which is currently
in use by Redundant Management. After the image update completes, Redundant
Management functionality will be unavailable until the system has been rebooted.

Continue (y/n)? y
Connected to 192.168.2.116.
Changing to: /C/Users/Administrator/.
sftp> get E:/Descargas/ArubaOS-CX_6200_10_06_0101.swi image.dnld.VmeRRh
Fetching /C/Users/Administrator/E:/Descargas/ArubaOS-CX_6200_10_06_0101.swi to
image.dnld.VmeRRh
/C/Users/Administrator/E:/Descargas/ArubaOS-C100%  338MB   5.6MB/s   01:00

Verifying and writing system firmware...
Aruba-CX(config)#
```

154. Si el *firmware* no es correcto devuelve un mensaje de error informando de su inconsistencia

```
Fetching /C/Users/Administrator/E:/Descargas/WC_16_10_0014.swi to image.dnld.4M8eMe
/C/Users/Administrator/E:/Descargas/WC_16_10_100%   29MB   6.6MB/s   00:04

Verifying and writing system firmware...
Firmware image signature is not valid
Aruba-CX(config)#
```

155. Para comprobar las versiones de software que se encuentran en cada partición se debe utilizar el siguiente comando:

```
Aruba-CX(config)# show images
```

156. Una vez copiado el software a la partición deseada con los comandos indicados, el producto llevará a cabo las modificaciones necesarias durante el siguiente arranque, por lo que **se recomienda reiniciar el dispositivo tras cada actualización**.

157. Para comprobar la vesión de software cargada actualmente utilizar el siguiente comando:

```
Aruba-CX(config)# show version
```

## 5.11 AUTO-CHEQUEOS

158. El producto realiza una comprobación del *firmware* durante el arranque. En caso de error, se cancela la ejecución y trata de ejecutar la versión de la otra partición. En caso que esta segunda falle, el sistema proporciona acceso al *ServiceOS* desde la consola, desde la que se podría proporciona una correcta versión.

```
Looking for SVOS.

Primary SVOS:  Checking...Loading...Finding...Verifying...Booting...

ServiceOS Information:
    Version:          ML.01.08.0002
    Build Date:       2021-02-19 08:02:23 UTC
```

```
    Build ID:         ServiceOS:ML.01.08.0002:04af6da43747:202102190802
    SHA:              04af6da43747146d6da5ab9ca4622efa65289a78

Boot Profiles:

0. Service OS Console
1. Primary Software Image [ML.10.06.0101]
2. Secondary Software Image [ML.10.07.0004]

Select profile(primary):

Booting primary software image...
Verifying Image...
Image Info:

        Name: ArubaOS-CX
     Version: ML.10.06.0101
    Build Id: ArubaOS-CX:ML.10.06.0101:f197b0b27572:202103010059
  Build Date: 2021-02-28 17:31:44 PST


Extracting Image...
Installing Rootfs...
Loading Image...
Done.
kexec_core: Starting new kernel
System is initializing
```

## 5.12 AUDITORÍA

### 5.12.1 REGISTRO DE EVENTOS

159. El equipo genera diferentes mensajes de *log*. Estos mensajes de *log* pueden inspeccionarse mediante el comando *show logging*.

```
switch# show logging ?
  -a    Display event logs from previous and current boots
  -c    Display event logs for specified event category
  -d    Display event logs for specified daemon
  -e    Display event logs for specified event IDs
  -i    Event logs for specified vsf member
  -m    Display event logs for specified vsf role
  -n    Display the specified number of event logs
  -r    Display event logs in reverse order (most recent first)
  -s    Display event logs as per specified severity
  <cr>
```

160. La descripción detallada de los mensajes generados se encuentra en el documento *AOS-CX Event Log Message Reference Guide* incluida en la documentación de cada producto (*REF4-REF11*).

161. Se muestra un ejemplo de salida de mensajes *log*:

```
switch# show logging -r
2022-04-22T12:06:34.227711+00:00 switch ops_mgmtintfcfg[3536]: Event|4301|LOG_INFO|AMM|-
|MGMT_INTF: Configured admin status up on Mgmt interface
2022-04-22T11:12:14.471352+00:00 switch hpe-restd[857]: Event|4650|LOG_INFO|AMM|-|Unable
to fetch Aruba Central location  from activate via VRF .
2022-04-22T11:12:14.469210+00:00 switch hpe-restd[857]: Event|4646|LOG_INFO|AMM|-|Aruba
Activate server https://devices-v2.arubanetworks.com is not reachable through any
supported VRF.
2022-04-22T11:07:58.464051+00:00 switch hpe-restd[857]: Event|4650|LOG_INFO|AMM|-|Unable
to fetch Aruba Central location  from activate via VRF .
```

```
2022-04-22T11:07:58.462065+00:00 switch hpe-restd[857]: Event|4646|LOG_INFO|AMM|-|Aruba
Activate server https://devices-v2.arubanetworks.com is not reachable through any
supported VRF.
2022-04-22T11:05:50.462483+00:00 switch hpe-restd[857]: Event|4650|LOG_INFO|AMM|-|Unable
to fetch Aruba Central location  from activate via VRF .
2022-04-22T11:05:50.460480+00:00 switch hpe-restd[857]: Event|4646|LOG_INFO|AMM|-|Aruba
Activate server https://devices-v2.arubanetworks.com is not reachable through any
supported VRF.
2022-04-22T11:04:46.465883+00:00 switch hpe-restd[857]: Event|4650|LOG_INFO|AMM|-|Unable
to fetch Aruba Central location  from activate via VRF .
2022-04-22T11:04:46.464319+00:00 switch hpe-restd[857]: Event|4646|LOG_INFO|AMM|-|Aruba
Activate server https://devices-v2.arubanetworks.com is not reachable through any
supported VRF.
2022-04-22T11:04:15.781171+00:00 switch ops_mgmtintfcfg[3536]: Event|4301|LOG_INFO|AMM|-
|MGMT_INTF: Configured admin status up on Mgmt interface
2022-04-22T11:04:15.734978+00:00 switch ops_mgmtintfcfg[3536]: Event|4301|LOG_INFO|AMM|-
|MGMT_INTF: Configured admin status up on Mgmt interface
2022-04-22T11:04:15.647286+00:00 switch ops_appsdnsclient[2869]:
Event|11901|LOG_INFO|||Dynamic domain name update event for VRF mgmt
2022-04-22T11:04:15.553061+00:00 switch ops_appsdnsclient[2869]:
Event|11901|LOG_INFO|||Dynamic domain name update event for VRF mgmt
2022-04-22T11:04:15.490276+00:00 switch ops_mgmtintfcfg[3536]: Event|4301|LOG_INFO|AMM|-
|MGMT_INTF:  Clearing the dhcp configuration due to link down (or) link remove.
2022-04-22T11:04:15.490183+00:00 switch ops_mgmtintfcfg[3536]: Event|4301|LOG_INFO|AMM|-
|MGMT_INTF: Netlink event down with message type 16 for management interface.
2022-04-22T11:04:15.418669+00:00 switch ops_appsdnsclient[2869]:
Event|11901|LOG_INFO|||Dynamic domain name update event for VRF mgmt
2022-04-22T11:04:15.323794+00:00 switch ops_mgmtintfcfg[3536]: Event|4303|LOG_CRIT|AMM|-
|MGMT_INTF: Link state is down.
2022-04-22T11:04:15.302701+00:00 switch ops_mgmtintfcfg[3536]: Event|4301|LOG_INFO|AMM|-
|MGMT_INTF: Configured admin status up on Mgmt interface
2022-04-22T11:04:14.481464+00:00 switch hpe-restd[857]: Event|4650|LOG_INFO|AMM|-|Unable
to fetch Aruba Central location  from activate via VRF .
2022-04-22T11:04:14.479195+00:00 switch hpe-restd[857]: Event|4646|LOG_INFO|AMM|-|Aruba
Activate server https://devices-v2.arubanetworks.com is not reachable through any
supported VRF.
switch#
```

162. En el documento *Diagnostics and Supportability Guide* de cada modelo se detallan la gestión de los eventos generados en el sistema (REF4-REF11)

### 5.12.2 ALMACENAMIENTO LOCAL

163. La rotación de registros permite al administrador del sistema rotar y archivar sistemáticamente los archivos de registro producidos por el sistema. La rotación de registros reduce la necesidad de espacio en disco del sistema operativo. La función utiliza la utilidad *Linux log-rotate* para la rotación de registros. La rotación de registros rota y comprime los archivos.

164. Por defecto, almacena localmente los ficheros. Se puede enviar los archivos de registro rotados a un equipo remoto mediante la configuración de un identificador universal de recursos (URI) de un  host remoto especificado mediante. **Esta funcionalidad solo permite utilizar el protocolo TFTP, por lo que no debe utilizarse**.

165. Por defecto, la función de rotación de registros rota los archivos de registro diariamente. Si el tamaño máximo del archivo supera los 100 MB, también se activa la rotación de registros. Cualquiera que sea la condición que ocurra primero (período o tamaño) activa la rotación de registros.

166. La rotación del registro no se produce inmediatamente después de que se alcance el tamaño máximo del archivo de registro, si no que se ejecuta con una periodicidad horaria.

167. Se puede fijar el tamaño del archivo que como se ha comentado, por defecto son 100 MB.

```
switch(config)# logrotate maxsize <10-200 MB>
```

168. También es posible cambiar la frecuencia de la rotación del fichero, que por defecto es diaria.

```
switch(config)# logrotate period {daily | hourly | weekly | monthly }
```

169. El conjunto de mensajes está formado por diferentes ficheros de logs. Estos pueden ser inspeccionados desde la *shell* de *ServiceOS*. Los únicos ficheros que rotan son los siguientes:

a) Registros de eventos almacenados en el archivo */var/log/event.log*.

b) Registros de autenticación almacenados en el archivo */var/log/auth.log*.

c) Registros de auditoría almacenados en el archivo */var/log/audit/audit.log*.

170. La rotación de *logs* puede inspeccionarse con el comando *show logrotate*

```
switch# show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 10MB
switch#
```

171. Los archivos de registro rotados se comprimen y se almacenan localmente en */var/log/*, accesible ese directorio desde *ServiceOS*. En circunstancias normales no es necesario acceder a dicha carpeta.

172. Los archivos de registro rotados se almacenan con la respectiva extensión de tiempo a la granularidad de la hora en el formato *file1-YYYMMDDHH.gz* (por ejemplo, *messages-2015080715.gz*). Los archivos de registro rotados se sustituyen cuando el número de archivos de registro rotados antiguos es superior a tres. El nuevo archivo de registro rotado sustituye al archivo de registro rotado más antiguo.

### 5.12.3 ALMACENAMIENTO REMOTO

173. El producto permite enviar los registros de auditoría a un servidor externo mediante *syslog*. El cliente *syslog* utiliza por defecto UDP para la comunicación, aunque también se admiten TCP y TLS. **Se deberá configurar el envío a un servidor externo de auditoría empleando TLS**.

174. Cuando se configura AOS-CX para enviar registros a un servidor remoto, es una práctica común establecer un valor de facilidad (*facility level*). Este valor actúa como una etiqueta que el servidor remoto puede utilizar para determinar qué archivo debe adjuntar el mensaje *syslog*.

175. Se deben seguir los siguientes pasos para configurar el envío de los registros a un servidor externo mediante TLS. Esta configuración hará uso de TLSv1.2 (la versión de TLS utilizada no es configurable):

- Configurar el servidor al que se enviarán los registros.

  *switch(config)# logging [<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>] tls <PORT-NUM> auth-mode subject-name include-auditable-events severity debug [vrf <VRF-NAME>]*

- Configurar el certificado (ver apartado 5.7 CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS) para ser usado por el cliente *syslog.*

  *switch(config-cert-name)# crypto pki application syslog-client certificate <CERT-NAME>*

- Asegurar la comprobación de SAN/CN con el siguiente comando.

switch(config)# crypto pki application syslog validate-cert-ext san-cn

## 5.13 *BACKUP*

### 5.13.1 CHECKPOINTS

176. Un *Checkpoint* es una instantánea de la configuración en ejecución de un conmutador y sus metadatos relevantes durante el tiempo de creación.

177. Los *Checkpoint* se pueden utilizar para aplicar la configuración del conmutador almacenada en un punto de control siempre que sea necesario, por ejemplo, para volver a una configuración anterior y limpia.

178. Los puntos de control solo pueden aplicarse a otros conmutadores de la misma familia.

179. El conmutador admite dos (2) tipos de puntos de control:

a) Puntos de control generados por el sistema: El conmutador genera automáticamente un punto de control del sistema cada vez que se produce un cambio de configuración.

b) Puntos de control generados por el usuario: El administrador puede generar manualmente un punto de control siempre que sea necesario.

180. Se recomienda realizar *Checkpoints* de forma periódica, de tal forma que en caso de fallo o error sea posible restaurar el estado del producto.

181. Dichos *Checkpoint* se almacenan localmente, por lo tanto se deberá utilizar el comando *copy checkpoint* para enviar estos ficheros a una ubicación externa y almacenarlos de forma segura. Tanto el envío desde el producto a un servidor, como la recuperación desde el servidor, se deberán hacer utilizando el protocolo SFTP.

182. El detalle de configuración de los *Checkpoint* se puede consultar en el apartado *Checkpoints* de la guía *AOS-CX 10.06 Fundamentals Guide – REF12*.

## 5.14 ALTA DISPONIBILIDAD

183. La alta disponibilidad de los equipos se proporciona mediante la constitución de chasis virtual o bien de stacks de equipos.

184. Los equipos de las familias 8300, 8400 y 6400 utilizan Aruba VSX. Las familias 6200 y 6300 utilizan Aruba VSF.

### 5.14.1 ARUBA VSX

185. Aruba VSX se caracteriza por la integración de dos equipos pasan a formar un equipo virtual. Cada miembro de los equipos mantiene su plano de control propio, y su autonomía operativa, pero sincronizan el estado de algunas de sus funciones para proporcionar una percepción que se trata de un solo equipo. En Aruba VSX a modo cada equipo tiene su propio direccionamiento.

186. En otras palabras, con Aruba VSX dos equipos se presentan en la red como un solo equipo a Nivel 2 pero como dos equipos a Nivel 3.

187. Las principales ventajas que aporta Aruba VSX son la alta disponibilidad y continuidad en el servicio, así como poder liberar de la necesidad de hacer usos de protocolos como *Spanning Tree* que se han demostrado problemáticos en la operación.

188. La decisión de hacer uso o no de Aruba VSX tiene por tanto un carácter de arquitectura y diseño funcional de la red. Las medidas de seguridad recomendadas son las mismas con VSX que un equipo individual.

189. El detalle de la configuración de VSX se puede consultar en el documento *AOS-CX Virtual Switching Framework (VSF) Guide* dentro de la documentación de las familias 6400, 8300 y 8400 (REF4, REF7–REF10).

### 5.14.2 ARUBA VSF

190. Aruba VSF es una tecnología de stack o apilamiento de equipos. Tiene la característica que se realiza por puertos de red estándar. Esto permite que los equipos agrupados puedan estar adyacentes o bien separados físicamente. Esto aporta sencillez a los diseños de red.

191. Aruba VSF hace que todos los equipos tengan se comporten como un equipo tanto a nivel 2 como a nivel 3, se ejecuta la misma versión de software en todos los equipos.

192. La decisión de hacer uso o no de Aruba VSF tiene por tanto un carácter de arquitectura y diseño funcional de la red. Las medidas de seguridad recomendadas son las mismas con VSF que un equipo individual.

193. El documento *AOS-CX Virtual Switching Framework (VSF) Guide* dentro de la documentación de las familias 6200 y 6300 (REF4 y REF5).

## 5.15 CONTROL DE ACCESO A LA RED

194. Los equipos permiten autenticar, autorizar y registrar los accesos a la red de los usuarios y dispositivos.

195. Una buena práctica es disponer que **todos los puertos de red habilitados, autentiquen a los dispositivos que se intenten conectar**. De esta forma, se evita que usuarios que tengan acceso físico a las dependecias de la organización, puedan conectar cualquier dispositivo sin autorización.

196. Para desplegar esta funcionalidad son necesarios tres pasos importantes:

    a) Configurar servidores RADIUS. Estos servidores recibirán todas las peticiones de autenticación. El detalle de configuración de los servidores RADIUS se puede consultar en el apartado *RADIUS General Tasks* de la guía *AOS-CX 10.06 Security Guide – REF13*.

    b) Configurar políticas de usuarios. Para cada tipo de usuario, dispositivo o estado, es posible configurar su política correspondiente para que posteriormente sea asignada. El detalle de configuración de las políticas se puede consultar en el apartado *Port Access policy* de la guía *AOS-CX 10.06 Security Guide – REF13*.

    c) Configurar los puertos para que realicen la autenticación. Para ello utilizar los siguientes comandos:

    *aaa authentication port-access dot1x authenticator enable*

    *aaa authentication port-access mac-auth enable*

197. En AOS-CX el comportamiento que se permite a los dispositivos conectados al equipo, es decir, las políticas que se aplican a cada dispositivo conectado, se puede regular con dos aproximaciones:

    a) Asignar la VLAN y definir filtros mediante ACL. El detalle de configuración de listas de acceso se puede consultar la guía *AOS-CX 10.06 ACLs and Clasiffier Policies Guide– REF14.*

    b) Asignar un rol de acceso. Este permite definir los permisos de acceso con mayor granularidad. El detalle de configuración de los roles se puede consultar en el apartado *Port Access role* de la guía *AOS-CX 10.06 Security Guide – REF13*.

198. Para más información sobre el control de acceso a la red, se recomienda consultar en el apartado *Port Access* de la guía *AOS-CX 10.06 Security Guide – REF13*.

## 5.16 RESETEO A FABRICA (*FACTORY DEFAULTS*)

199. En caso necesario, es posible devolver los dispositivos a un estado de fábrica. El método recomendado es ponerlo a cero. Cuando se inicia el proceso de puesta a cero ocurre lo siguiente:

    a) El conmutador se reinicia a *ServiceOS*.

b) Los archivos de imagen de software primario y secundario se respaldan en la memoria desde el almacenamiento flash.

c) Todo el dispositivo de almacenamiento *flash* se sobrescribe con ceros para borrar de forma segura todos los datos almacenados.

d) El dispositivo de almacenamiento *flash* se reformatea con un sistema de archivos predeterminado de fábrica.

e) Los archivos de imagen de *software* respaldados se escriben en flash en sus ubicaciones originales.

f) El conmutador se reinicia a la imagen de *software* primaria con una configuración predeterminada.

200. Hay cuatro (4) métodos que se pueden utilizar para poner a cero un *switch*.

201. En primer lugar, un usuario administrador puede utilizar el comando *erase all zeroize* de la CLI del AOS-CX:

```
switch# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.

Continue (y/n)?
```

202. En segundo lugar, y para equipos 6400 o 8400 un usuario administrador puede utilizar el comando *erase zeroize* desde la CLI de *ServiceOS*, para borrar de forma segura cualquier dato del usuario contenido en el SSD u otros dispositivos de almacenamiento del módulo de gestión:

*SVOS> erase zeroize*

*################################WARNING################################*

*This will securely erase all customer data and reset the switch*

*to factory defaults. This will initiate a reboot and render the*

*switch unavailable until the zeroization is complete.*

*This should take several minutes to one hour to complete.*

*################################WARNING################################*

*Continue (y/n)?*

203. En tercer lugar, un usuario con acceso físico al panel frontal del conmutador y a un dispositivo de almacenamiento USB con formato *FAT32* puede poner a cero el conmutador (el USB se usa a modo de verificar el acceso físico al equipo, equivalente a un hipotético botón de reset que no existe). Desde el prompt de inicio de sesión de ServiceOS introduciendo el nombre de usuario *zeroize* y siguiendo las instrucciones proporcionadas:

```
ServiceOS login: zeroize

This will securely erase all customer data, including passwords, and
reset the switch to factory defaults.
```

```
This action requires proof of physical access via a USB drive.
* Create a FAT32 formatted USB drive
* Create a file in the root directory of the USB drive named zeroize.txt
* Type the following serial number into the zeroize.txt file: xxxxxxxxxx
* Insert the USB drive into the target module
* Confirm the following prompt to continue

Continue (y/n)?
```

204. Por último, tal como se indica en el apartado 5.2 MODO DE OPERACIÓN SEGURO, al cambiar el modo de seguridad del conmutador, este se pone a cero.

## 5.17 MITIGACION DE ATAQUES

### 5.17.1 *DHCP SNOOPING*

205. *DHCP snooping* protege la red de los ataques DHCP más comunes, como la suplantación de direcciones resultante de un servidor DHCP fraudulento que opera en la red, o el agotamiento de las direcciones en un servidor DHCP causado por las solicitudes masivas de direcciones de un atacante en la red. La utilidad funciona designando servidores DHCP de confianza y puertos en los que se aceptarán las solicitudes y respuestas DHCP. **Se debe activar DHCP snooping**.

206. DHCP snooping se soporta en los modelos 6200, 6300, 6400 y 8400.

207. Para determinar los servidores DHCP autorizados o de confianza se usa el comando *dhcpv4-snooping*. Se muestra un ejemplo, donde se muestra cómo configurarlo por VRF.

*switch(config)# dhcpv4-snooping authorized-server 192.168.2.2*

*switch(config)# dhcpv4-snooping authorized-server 192.168.2.3 vrf default*

*switch(config)# dhcpv4-snooping authorized-server 192.168.2.10 vrf default*

208. Para activar la funcionalidad, en un puerto o en una vlan se usa el comando *dhcpv4-snooping.*

```
Ejemplo de configuración por interfaz
switch(config)# interface 1/1/1
switch(config-vlan-100)# dhcpv4-snooping
switch(config-vlan-100)# exit
```

*switch(config)#*

```
Ejemplo de configuración por vlan
switch(config)# vlan 100
switch(config-vlan-100)# dhcpv4-snooping
switch(config-vlan-100)# exit
```

*switch(config)#*

209. Existen más parámetros de la funcionalidad, disponibles en el manual *AOS CX IP Services* (REF4-REF11).

### 5.17.2 *DYNAMIC ARP INSPECTION*

210. El Protocolo de Resolución de Direcciones (ARP) permite a los hosts comunicarse a través de la red creando un mapeo de direcciones IP a MAC que se utiliza en la transmisión de paquetes. Los atacantes pueden utilizar ARP para generar mapeos falsos, lo que les permite falsificar las direcciones MAC de otros clientes e interceptar el tráfico destinado a ellos. Además, un atacante podría generar un número ilimitado de entradas ARP artificiales, llenando las cachés de otros clientes en la red y provocando una denegación de servicio (DoS).

211. El comando *arp inspection* activa la inspección dinámica de ARP en la VLAN actual, obligando a que todos los paquetes ARP procedentes de puertos no confiables sean sometidos a una comprobación de asociación MAC-IP contra una tabla de vinculación. **Se debe activar esta funcionalidad.**

212. El tamaño de la tabla dinámica se puede configurar con el comando *arp cache-limit.*

213. La activación de la funcionalidad se hace por VLAN.

*switch(config)# arp cache-limit 4097*

*switch(config)# vlan 1*

*switch(config-vlan)# arp inspection*

214. La inspección dinámica de ARP se soporta en 6200, 6300, 6400 y 8400. Existen más parámetros de la funcionalidad, disponibles en el manual *AOS CX IP Services* (REF4-REF11)

### 5.17.3 *CONTROL PLANE POLICING*

215. La vigilancia del plano de control (CoPP) evita que la inundación de ciertos tipos de paquetes sobrecargue la CPU del conmutador o del módulo limitando la velocidad o descartando los paquetes. El *software* del conmutador proporciona un número de clases configurables de paquetes que pueden ser limitados en su velocidad, incluyendo (pero no limitado a) las difusiones ARP, la multidifusión, los protocolos de enrutamiento (BGP, OSPF) y el árbol de expansión.

216. El producto dispone de una política de CoPP por defecto. Esta puede modificarse, pero no eliminarse. En caso de querer revertir a la política por defecto, utilizar el siguiente comando:

*switch(config)# copp-policy default revert*

217. El detalle de configuración de la vigilancia de control de plano se puede consultar en el apartado *Control Plane Policing (CoPP)* de la guía *AOS-CX 10.06 Fundamentals Guide – REF12*.

## 5.18 PROTOCOLOS DE *ROUTING*

### 5.18.1 BGP

218.A continuación se indican prácticas de seguridad en el empleo del protocolo BGP.

219.BGP es soportado en las plataformas 6300, 6400, 8320, 8325, 8360 y 8400.

#### 5.18.1.1 ACL DEL PLANO DE CONTROL PARA LAS SESIONES DE *PEERING* DE BGP

220.Los dispositivos que ejecutan BGP escuchan conexiones en el puerto TCP 179. Al establecer una sesión de *peering* BGP, un dispositivo establecerá activamente una relación con el otro *peer* enviando el primer paquete TCP SYN. Este dispositivo se conoce como el lado saliente de la conexión. El otro *peer*, al escuchar el TCP SYN, responde con un SYN/ACK, es referido como la conexión entrante. Dado que cualquiera de los dos *peers* puede asumir cualquiera de los dos papeles, es necesario configurar entradas ACL para BGP en ambas direcciones.

221.Por ejemplo, las siguientes entradas permitirán el tráfico desde 10.20.0.10 para que pueda establecer una sesión de *peering* BGP con el dispositivo. Dado que cualquiera de los dos lados puede jugar el papel de salida o de entrada en la conexión, la ACL requiere dos entradas por peer:

*switch(config)# access-list ip CONTROLPLANE*

*switch(config-acl-ip)# 800 comment LOCKDOWN BGP SESSIONS*

*switch(config-acl-ip)# 805 permit tcp 10.20.0.10 gt 1023 any eq 179*

*switch(config-acl-ip)# 810 permit tcp 10.20.0.10 eq 179 any gt 1023*

222.Después de permitir el tráfico de todos los *peers* configurados, bloquear todos los demás dispositivos para que no puedan intentar establecer una sesión de peering BGP, denegando el resto del tráfico hacia o desde el puerto TCP 179.

*switch(config-acl-ip)# 890 deny tcp any gt 1023 any eq 179*

*switch(config-acl-ip)# 895 deny tcp any eq 179 any gt 1023*

#### 5.18.1.2 AUTENTICACIÓN DE *PEERS* BGP

223.Las sesiones TCP entre los dos *peers* pueden asegurarse añadiendo protección a la cabecera de la sesión TCP. Esta actúa como una contraseña entre los *peers*. Esta configuración se realiza dentro del contexto de configuración de BGP, y ambos *peers* deberán configurar la misma contraseña.

*switch(config-bgp)# neighbor 10.20.0.10 password plaintext contraseña*

#### 5.18.1.3 SEGURIDAD DEL TTL DE BGP

224.Asumiendo que la mayoría de los vecinos de enrutamiento están típicamente conectados directamente, un método simple para bloquear la suplantación remota

desde dispositivos remotos es verificar el *Time to Live* (TTL) de los paquetes del *peer* y descartar los paquetes cuyo TTL es menor que la cantidad esperada.

225. Se muestra un ejemplo usando el peer BGP especificado anteriormente. Asumiendo que el valor máximo de TTL es 255, los paquetes del *peer* se comparan con el *hop-count*, introducido abajo como un valor de 1.

*switch(config-bgp)# neighbor 10.20.0.10 ttl-security-hops 1*

226. Con un valor máximo de TTL de 255 y un valor configurado de *hop-count* de 1, los paquetes con un TTL inferior a 254 serán descartados.

#### 5.18.1.4 OTRAS CONFIGURACIONES DE BGP

227. Para elementos adicionales relacionados con BGP, como la configuración del filtrado de rutas entrantes y salientes o la limitación del número máximo de rutas a aprender por vecino BGP, consultar los apartados *BGP* y *Políticas de Ruta y Mapas de Ruta* de la guía de *AOS-CX IP Routing Guide* (REF4, REF7-REF11).

### 5.18.2 OSPF

#### 5.18.2.1 INTERFACES PASIVAS OSPF

228. OSPF es soportado en las plataformas 6200, 6300, 6400, 8320, 8325, 8360 y 8400.

229. A diferencia de BGP, la mayoría de los protocolos de enrutamiento tienden a descubrir vecinos mediante el envío y la recepción de paquetes *Hello*. Debido a que la construcción de estas relaciones de vecindad ocurre dinámicamente, el administrador debe tomar medidas para controlar dónde se pueden formar las relaciones de vecindad y que los vecinos potenciales sean dispositivos conocidos y de confianza.

230. Para limitar dónde puede aprender vecinos OSPF, AOS-CX soporta el concepto de interfaces OSPF pasivas. Una interfaz OSPF pasiva tiene sus subredes IP anunciadas, pero no establece relaciones de vecinos con otros dispositivos OSPF en la interfaz.

231. **El método recomendado es hacer pasivas todas las interfaces OSPF habilitadas**:

*switch(config-ospf-10)# passive-interface default*

232. La interfaz pasiva es entonces removida de cada interfaz específica donde las relaciones de vecinos OSPF son permitidas. Como este es un cambio de configuración a nivel de interfaz, ocurre desde el contexto de la interfaz:

*switch(config-if)# no ip ospf passive*

#### 5.18.2.2 AUTENTICACIÓN DE VECINOS OSPF

233. AOS-CX soporta varios métodos de autenticación OSPF, incluyendo hashes criptográficos SHA de hasta 512 bits, para autenticar mensajes entre vecinos OSPF. Al configurar la autenticación entre vecinos OSPF, el método de autenticación y la clave deben ser los mismos en las interfaces conectadas en ambos dispositivos.

234. **Se recomienda configurar la autenticación SHA-512**. Para ello cambiar el método de autenticación por defecto de *null* a *hmac-sha-512* desde el contexto de la interfaz:

*switch(config-if)# ip ospf authentication hmac-sha-512*

235. A continuación, configurar una clave SHA que se utilizará para la conexión; la clave puede introducirse como texto plano o como una cadena de texto cifrado con hash:

*switch(config-if)# ip ospf sha-key 1 plaintext ospfshakeystring*

236. Cualquier clave introducida en texto plano será automáticamente cifrada antes de ser almacenada en la configuración del switch.

237. Alternativamente, la función de llavero de AOS-CX puede ser utilizada para especificar una clave de autenticación criptográfica a nivel de sistema que puede ser utilizada por múltiples interfaces OSPF:

*switch(config)# keychain ospf-keychain*

*switch(config-keychain)# key 1*

*switch(config-keychain-key)# cryptographic-algorithm hmac-sha-512*

*switch(config-keychain-key)# key-string plaintext ospfshakeystring*

*switch(config-keychain-key)# interfaz 1/1/49*

*switch(config-if)# ip ospf authentication keychain*

*switch(config-if)# ip ospf keychain ospf-keychain*

#### 5.18.2.3 AUTENTICACIÓN Y CIFRADO DE ÁREA *OSPFV3* CON IPSEC

238. La configuración de autenticación o cifrado de área *OSPFv3* será anulada por la autenticación o cifrado a nivel de interfaz, donde esté configurada.

239. Los vecinos de OSPFv3 pueden utilizar la autenticación a nivel de interfaz, como se describe en la sección anterior. Sin embargo, se puede utilizar un método alternativo para proporcionar cifrado y/o autenticación para toda un área OSPFv3 utilizando el protocolo IPsec, que aplica automáticamente los métodos configurados a todas las interfaces miembros.

240. Hay dos (2) tipos de encapsulación IPsec soportados en AOS-CX para asegurar áreas OSPFv3:

a) Cabecera de autenticación IPv6 (AH), que añade una cabecera de autenticación IPv6 a los paquetes OSPFv3.

b) *Encrypted Security Payload* (ESP), que proporciona tanto autenticación como cifrado para los paquetes OSPFv3.

241. La autenticación y el cifrado IPsec se configuran desde el contexto del proceso del router OSPFv3:

switch(config)# router ospfv3 1

switch(config-ospfv3-1)#

242. Tanto la autenticación como el cifrado requieren un índice de política de seguridad (SPI) especificado, que es un valor entero entre 256 y 4.294.967.295; este valor se utiliza en cada router OSPFv3 en el área asegurada para coincidir con una política de autenticación y/o cifrado IPsec configurada.

243. Cada política IPsec OSPFv3 en un conmutador debe utilizar un valor SPI diferente, y el valor SPI (así como las claves de autenticación y/o cifrado) debe coincidir en todas las interfaces vecinas OSPFv3 que utilicen esa política dentro del área asegurada.

244. Para configurar la autenticación AH para el área 1 de OSPFv3, especificar el SPI, el método de autenticación (seleccionar el de mayor fortaleza posible), el tipo de clave (texto plano, cadena hexadecimal o texto cifrado) y la propia cadena de claves. Si no se especifica un tipo de clave y una cadena, se pedirá al usuario que introduzca una clave de texto plano de forma interactiva:

*switch(config-ospfv3-1)# area 1 authentication ipsec spi 1024 sha1*

*Enter the IPsec authentication key: *******

*Re-Enter the IPsec authentication key: ********

245. Para configurar el cifrado ESP para el área 1, especificar el SPI, el método de autenticación, el tipo y la cadena de la clave de autenticación, el tipo de cifrado (seleccionar aes), el tipo de clave y la cadena de la clave de cifrado. Si no se especifican el tipo de cifrado y la cadena de claves, se pedirá al usuario que introduzca una clave en texto plano de forma interactiva.

246. Si el tipo y la cadena de clave de autenticación no se especifican, se pedirá al usuario que introduzca tanto una clave de autenticación en texto plano como el tipo de cifrado y la clave en texto plano deseados.

*switch(config-ospfv3-1)# area 1 encryption ipsec spi 1024 sha1*

*Enter the IPsec authentication key: *******

*Re-Enter the IPsec authentication key: *******

*Enter the IPsec encryption type (3des/aes/des/null)? aes*

*Enter the IPsec encryption key: ****************

*Re-Enter the IPsec encryption key: ****************

## 6. FASE DE OPERACIÓN

247. Durante la fase de operación se recomienda realizar las siguentes tareas periódicas:

- **Comprobar del *hardware* y *software*** para asegurar que no se ha introducido *hardware* o *software* no autorizado.
- **Realizar copias de seguridad con regularidad**, utilizando los *checkpoint* tal como se ha indicado.
- **Monitorizar el equipo**, revisando los eventos y logs de auditoría periódicamente.
- **Aplicar los parches de seguridad**.

## 7. CHECKLIST

| ACCIONES | SÍ | NO | OBSERVACIONES |
|---|---|---|---|
| **DESPLIEGUE E INSTALACIÓN** | | | |
| Verificación de la integridad del paquete | ☐ | ☐ | |
| Instalación física | ☐ | ☐ | |
| **CONFIGURACIÓN** | | | |
| **MODO DE OPERACIÓN SEGURO** | | | |
| Activación del modo *enhanced security* | ☐ | ☐ | |
| **ADMINISTRACIÓN DEL PRODUCTO** | | | |
| Configuración de usuarios y grupos | ☐ | ☐ | |
| Configuración de la política de contraseñas | ☐ | ☐ | |
| Configuración de los parámetros de sesión | ☐ | ☐ | |
| Configuración de la sincronización | ☐ | ☐ | |
| Configuración del banner de acceso al sistema | ☐ | ☐ | |
| **CONFIGURACIÓN DE PROTOCOLOS Y SERVICIOS SEGUROS** | | | |
| Deshabilitación de *HTTPS*, *Bluetooth*, *SNMP* y *Aruba Central* | ☐ | ☐ | |
| Configuración de los parámetros de SSH | ☐ | ☐ | |
| **CONFIGURACIÓN DE PUERTOS** | | | |
| Desactivación los puertos no utilizados | ☐ | ☐ | |
| **GESTIÓN DE CERTIFICADOS** | | | |
| Importar CA, crear CSR e importar el certificado de servidor | ☐ | ☐ | |
| **BACKUP** | | | |
| Creación de *Checkpoints* | ☐ | ☐ | |
| **CONTROL DE ACCESO A LA RED** | | | |

| ACCIONES | SÍ | NO | OBSERVACIONES |
|---|---|---|---|
| Configuración de la autenticación en los puertos | ☐ | ☐ | |
| **MITIGACIÓN DE ATAQUES** | | | |
| Activación *DHCP Snooping* | ☐ | ☐ | |
| Activación *Dynamic ARP Inspection* | ☐ | ☐ | |
| Activación *Control Plane Policing* | ☐ | ☐ | |
| **AUDITORÍA** | | | |
| Configuración del envío de los logs a un servidor *Syslog* | ☐ | ☐ | |
| **OPERACIÓN** | | | |
| Comprobación *hardware/sofware* | ☐ | ☐ | |
| Realización de copias de seguridad | ☐ | ☐ | |
| Monitorización del equipo | ☐ | ☐ | |
| Instalación de parches de seguridad | ☐ | ☐ | |

## 8. REFERENCIAS

248. Los documentos referenciados son documentos PDF empaquetados y que contienen diversos manuales. Es necesario la aplicación *Adobe Acrobat Reader* para su consulta. En todo caso, todos los manuales también se encuentran en *Aruba Support Portal* (REF1).


| | | |
|---|---|---|
| **REF1** | | Portal de soporte, documentación, licenciamiento, notificaciones de seguridad y otras funciones.<br>*Aruba Support Portal* https://asp.arubanetworks.com |
| **REF2** | | Aplicación Aruba CX Apple Store<br>https://apps.apple.com/us/app/aruba-cx/id1414572411 |
| **REF3** | | Aplicación Aruba CX Google Play<br>https://play.google.com/store/apps/details?id=com.arubacx&hl=en_US&gl=US |
| **REF4** | **6300**<br>**6400** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_6300-6400.pdf |
| **REF5** | **6200** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_6200.pdf |
| **REF6** | **6100**<br>**6000** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_6000-6100.pdf |
| **REF7** | **8400** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8400.pdf |
| **REF8** | **8360** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8360.pdf |
| **REF9** | **8325** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8325.pdf |

| | | |
|---|---|---|
| **REF10** | **8320** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_8320.pdf |
| **REF11** | **i4100** | Manuales producto<br>*Documentation Portfolio for 10.08*<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.08/PDF/pdf_port_4100i.pdf |
| **REF12** | **6300**<br>**6400** | AOS-CX 10.06 Fundamentals Guide<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7694/index.html#book.html |
| **REF13** | **6300**<br>**6400** | AOS-CX 10.06 Security Guide<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7723/index.html |
| **REF14** | **8320**<br>**8325** | AOS-CX 10.06 ACLs and Classifier Policies Guide<br>https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7679/index.html#book.html |

## 9. ABREVIATURAS

| | |
|---|---|
| **ACL** | *Access Control List* |
| **ARP** | *Address Resolution Protocol* |
| **CA** | *Certificate Authority* |
| **CLI** | *Command-Line Interface* |
| **CPD** | *Centro de Proceso de Datos* |
| **CPU** | *Central Processing Unit* |
| **DHCP** | *Dynamic Host Configuration Protocol* |
| **DNS** | *Domain Name System* |
| **ENS** | *Esquema Nacional de Seguridad.* |
| **HTTP** | *HyperText Trasfer Protocol* |
| **HTTPS** | *HyperText Trasfer Protocol Secure* |
| **MAC** | *Media Access Control* |
| **NAE** | *Network Analytics Engine* |
| **NTP** | *Network Time Protocol* |
| **OOBM** | *Out Of Band Management* |
| **OS** | *Operating System* |
| **SFTP** | *Secure File Transfer Protocol* |
| **SNMP** | *Simple Network Management Protocol* |
| **SSH** | *Secure SHell* |
| **TCP** | *Transmission Control Protocol* |
| **TFTP** | *Trivial File Transfer Protocol* |
| **TLS** | *Transport Layer Security* |
| **ZTP** | *Zero Touch Provisioning* |

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL